基于区块链的医疗电子病历大数据共享方案

刘曙霞[1]，杨斯博[2]，王琰[1]，杨爽[1]，王雅晴[1]，胥美美[1]，安新颖[1]
（[1]中国医学科学院医学信息研究所 北京 100020 [2]天津大学管理与经济学部 天津 300072）

摘要：[目的/意义]为解决传统电子病历大数据资源交互性差、安全性低等问题，提出具有去中心化、不可篡改以及加密机制的基于区块链的医疗电子病历大数据共享方案。[方法/过程]首先，分析当前区块链技术在医疗领域的应用；然后，采用问卷调查法和访谈法收集医疗市场对电子病历的需求；在此基础上，结合不对称加密技术、共识机制、智能合约等机制，提出五层次的基于区块链技术的医疗电子病历大数据资源共享方案。[结果/结论]该方案重塑医疗大数据资源共享流程，进一步完善区块链在医疗数据安全存储共享方面的应用，可为相关企业医院和研究者提供参考。

关键词：区块链技术 医疗大数据 电子病历 共享机制 系统设计
分类号：TP399

Sharing Solution for Electronic Medical Record Based on Block-chain in Big Data Environment

LIU Shu-xia[1] YANG Si-bo[2] WANG Yan[1] YANG Shuang[1] WANG Ya-qing[1] XU Mei-mei[1] AN Xin-ying[1]
（[1]Institute of Medical Information, Chinese Academy of Medical Sciences, Beijing 100020, China; [2]Tianjin University, Tianjin 300072, China）

Abstract:[Purpose/Significance]In order to address the issues of poor interactivity and low security in traditional electronic medical record big data resources, this paper proposes a blockchain-based electronic medical record big data sharing solution that is decentralized, tamper-proof, and encrypted.[Method/Process]Firstly, the application of current blockchain technology in the medical field is analyzed. Then, the demands for electronic medical records in the medical market are collected through questionnaire surveys and interviews. Based on this, a five-level blockchain-based electronic medical record big data resource sharing solution is proposed, which incorporates mechanisms such as asymmetric encryption technology, consensus mechanism, and smart contracts.[Results/Conclusions]This solution reshapes the process of sharing medical big data resources and further improves the application of blockchain in the secure storage and sharing of medical data. It can serve as a reference for relevant companies, hospitals,

作者简介：刘曙霞，硕士研究生在读，E-mail:liushuxia0420@163.com；杨斯博，副教授，博士；王琰，硕士研究生在读；杨爽，硕士研究生在读；王雅晴，硕士研究生在读；胥美美，副研究员，博士，E-mail:xumeimei2005@163.com；安新颖，研究员，博士。

and researchers.

Key words: Block-chain Technology; Medical Big Data; Electronic Medical Record; Sharing Mechanism; System Design

目前，区块链已经应用于医疗信息领域，并且其核心应用技术优势正日益凸显。国内外有很多区块链医疗应用的成功案例，如 IBM Waston 与 FDA 签署的基于区块链共享病人数据的项目协议，通过使用区块链技术设计和创建网络，提高医疗保健行业的透明度和互操作性；阿里健康与常州市合作“医联体+区块链”试点项目，旨在利用区块链技术保证部分医疗机构之间安全、可控的数据互联互通。

近年来，国内外也有不少区块链在医疗信息存储方面应用的研究。Ekblaw 等[1]提出去中心化电子病历管理系统 MedRec，Xiao Yue 等[2]提出使用区块链技术设计的数据共享架构－Healthcare Data Gateways。以上研究缺少具体的实施机制和操作流程。Shrier 等[3]提出基于具体机制的医疗数据保护方案，即基于麻省理工学院研发的 OPAL/Enigma 加密平台，使用区块链技术建立一个安全的医疗环境以存储分析医疗数据，但操作起来效率极低。为了在保护数据安全的同时提升效率，徐建等[4]提出基于智能合约的区块链网络医疗记录安全储存访问方案，能够帮助快速识别不利于保护数据完整性的行为，但其仅仅针对云端数据，未能解决数据源头的安全性问题。而 BitHealth[5]基于点对点的传播文件方式，实现区块链对医疗健康数据的存储保护，解决了安全性问题，但是在资源利用方面仍存在一些缺陷。

为了进一步完善区块链技术在医疗数据安全保护与共享方面的应用，本文提出五层次的基于区块链的医疗大数据资源共享方案，通过不对称加密技术在数据层实现对医疗数据的加密存储并采用 H.235 加密协议确保不同功能节点中信息共享的安全。同时为了保证资源充分利用，通过网络层的 P2P 协议联系不同终端，通过采取共识机制和智能合约，使不同医院的医生和患者可以快速安全地共享医疗数据。

1 医疗大数据电子病历特征分析

1.1 传统电子病历的发展

2023 年 2 月，中国医院协会信息管理专业委员会发布了《2021-2022 年度中国医院信息化状况调查报告》，其对全国 1062 家医院进行了调研，调查结果显示，参加电子病历系统功能应用水平分级评价的医院占调查总量的 96.14%，其中三级医院参加电子病历系统应用水平分级评价的比例达到 97.81%，说明多数医院已参与电子病历系统功能应用水平分级。将本年度电子

病历系统功能应用水平分级数据与2019-2020年度以及2018-2019年度的调查数据对比可见，参与电子病历系统功能应用水平分级的医院逐年增加，且参评等级逐年提高。2018—2019年评级通过占比最高的是3级，而2019—2020年则为4级占比最高，且比例逐年提高。这体现了医院电子病历系统功能的逐渐成熟。

根据我国卫生部《电子病历基本架构与数据标准》，电子病历是由医疗机构以电子化方式创建、保存和使用的，重点针对门诊、住院患者（或保健对象）临床诊疗和指导干预信息的数据集成系统（图1），是居民个人在医疗机构历次就诊过程中产生和被记录的完整、详细的临床信息资源。电子病历中一般包括医疗机构信息、门诊病历记录、法定医学证明及报告、住院病历记录等信息[6]。

与纸质病历相比，电子病历可以有效提高工作效率，提升医疗质量。然而，传统的医疗电子病历存在许多问题，比如无法对数据进行统一管理，患者在不同地区、不同医院的医疗就诊数据无法共享；电子病历中不少数据涉及患者的个人隐私，目前电子病历记录存储方式安全性低，数据很容易泄露或者被篡改等。



图1 传统医疗电子病历信息

1.2 医疗行业大数据化趋势

随着医疗行业信息化的建设，大部分的病历数据和临床数据都已经信息化，数据量的大规模增加给数据的存储和管理带来很大挑战。如图2所示，医疗行业大数据采集有多种渠道，从医疗信息系统（HIS）、电子病历系统（EMRS）、实验室信息系统（LIS）、医学影像存档与通信系统（PACS）、放射信息管理系统（RIS）、临床决策支持系统（CDSS）等信息系统中可以获取海量结构化数据和非结构化数据[7]，智能可穿戴健康设备的发展也使收集公众行为健康数据变得更为简单。

医疗大数据不仅具有规模大、类型多、时效性、准确性、价值高等传统大数据的特征，还具有不完整性、冗余性、隐私性等特征[8]。大规模的数据如果能够通过集中和共享得到有效利用，那将势必给医疗行业的发展带来前所未有的机遇和发展。

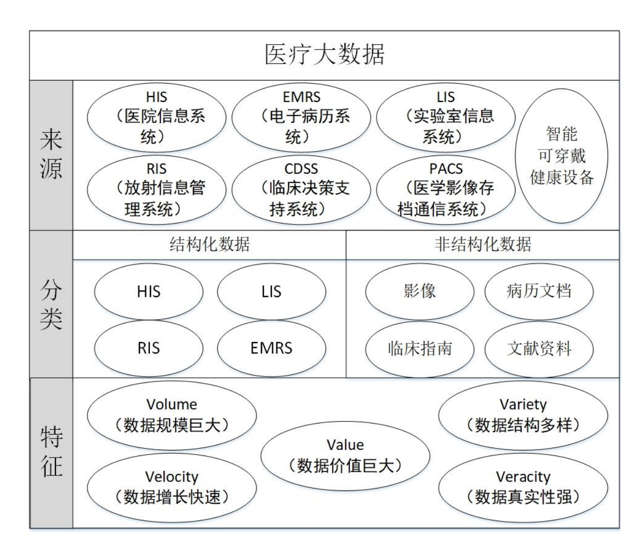


图 2 医疗行业大数据化

2 我国当前医疗电子病历数据共享情况调研分析

2.1 医疗数据共享情况调研

为了解医生和患者对医疗资源共享的需求，我们走访天津市 4 家三甲医院，包括天津市第一中心医院、天津市南开医院、天津医科大学总医院和天津市中医药大学附属第一医院，对医生和患者进行访谈。根据访谈得到的信息设计调查问卷，面向全国医生和患者开展调查，共回收信度效度较高的有效问卷 329 份，覆盖全国 24 个省市和地区（图 3）。329 份有效问卷中，医生回复的问卷占比为 15%。问卷结果显示，75%以上的医生（图 4）和 55%以上的患者（图 5）对现有医疗资源不够满意，经济落后的地区满意度更低，这在一定程度上显示出我国当前医疗资源匮乏、资源分配不均的问题十分严重。建设大型医疗数据共享平台不仅可以加快落后地区医疗行业的发展，还能将医疗数据库中的海量数据用于科研，创造更大的价值。

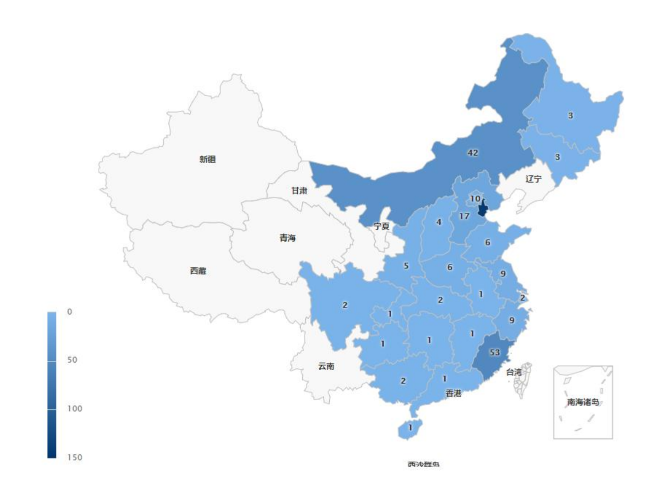


图 3 医疗资源满意度调查有效问卷的地区分布

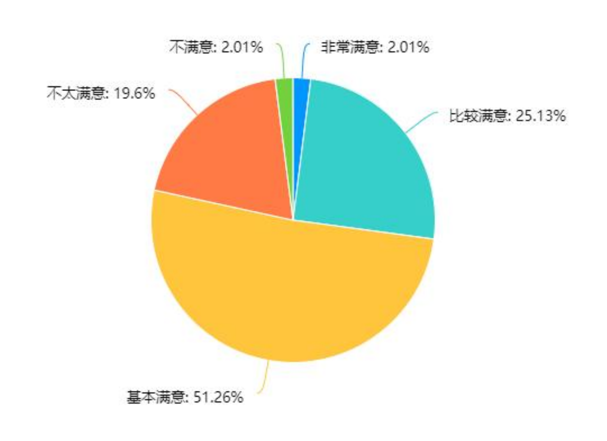


图 4 医生医疗资源满意度调查结果统计

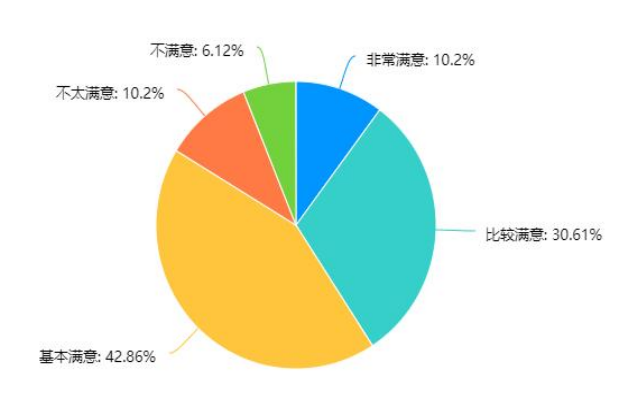


图 5 患者医疗资源满意度调查结果统计

2.2 建立电子病历档案

电子病历的普及提高了医院工作效率，但是其安全性差、数据信息中心化、访问权限不明确、限制患者知情权等问题也很突出。医疗信息反映了患者的健康状况，患者应该拥有知情权，但我们在调研时了解到，电子病历的中心控制权在医院，患者只能以打印的方式带走病历。虽然每个医院都有保护患者隐私的义务，但医院存储电子病历的系统极易被黑客入侵。另外，现有的电子病历系统只能记录患者单次的就诊信息，对于需要转院的慢性病患者或者病情与病史相关的患者，不完整的就诊记录会给后续治疗带来许多不便。为解决上述问题，我们提出建立基于区块链的电子病历档案，利用区块链分布式账本的特点，为每个患者建立记录每次就诊信息的电子病历档案，患者拥有自己档案的私钥和公钥，可以随时查看以及增加记录，而区块链去中心化、非对称加密算法的特点保障了电子病历档案的安全性。

3 基于区块链技术的医疗电子病历大数据资源共享方案设计与应用

3.1 系统体系框架设计

区块链技术是底层技术，具有普适性。一般来说，区块链系统由数据层、

网络层、共识层、激励层、合约层和应用层组成。数据层主要用来存储经过哈希加密的医疗大数据，网络层通过 P2P 协议将系统中的所有终端联系起来，共识层封装了不同节点之间的共识机制，激励层设计发行机制和分配机制，合约层封装了交易双方签署后的智能合约，应用层主要是系统使用者可直接进行操作的客户端（图 6）。

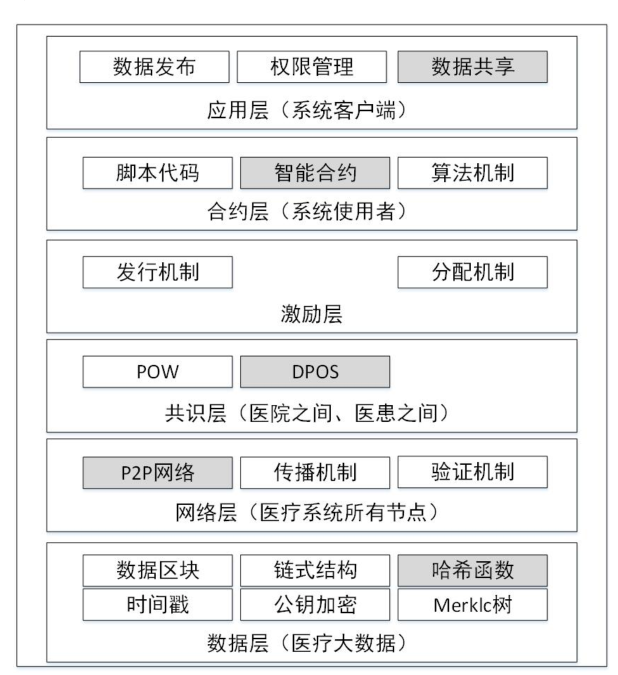


图 6 基于区块链的医疗大数据资源共享系统基础架构

针对基于区块链技术的医疗电子病历大数据共享系统设计要求，从各方面需求来看，系统应从医生与医生之间、医生与患者之间两方面利用区块链技术的去中心化、开放透明、可信安全等特点对现有的医疗系统进行创新，并利用分布式账簿的特点，完善现有的数据共享平台中的安全性问题与远程医疗信息交互的障碍。主要手段是通过不对称加密技术的应用，区分公钥与私钥各自可以实现的功能，以保证每一个节点中不同的功能的实现，进而实现数据在区块链上的交互，实现安全数据共享。

3.2 系统交互机制设计

3.2.1 医生与患者在就诊过程中信息交互的系统设计

在系统中，每一个区块记载着患者自身的病史记录，其中患者凡在区块链涵盖的医院范围内进行就诊的记录皆可保存在区块链中，利用密钥对其进行加密处理。患者可随时利用自己的公钥对自己以往的病史、病例、诊断记录等相关信息进行查看。

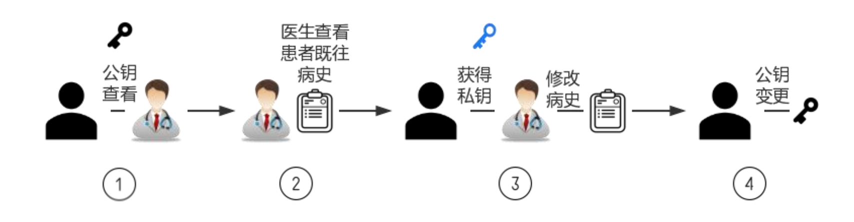


图 7 医生与患者就诊过程系统使用流程图

其过程可用算法 1 表示：

算法 1：患者就诊交互

```
1)Begin
2)While（患者挂号成功）
3) If（账户状态正常 and 验证    secret_key_doctor）
4)  {允许登录；获取权限；
5)   If（查看既往病史）
6)    readin(public_key_patient);
7)     验证 public_key_patient;
8)      If（验证通过）
9)        {获取查看权限;}
10)    If(add new_record)
11)     readin(secret_key_patient);
12)      验证 secret_key_patient;
13)      If（验证通过）
14)        {将新记录添加至患者区块:
15)        Add
new_record(doctor_ID||Sign(Hash(Data)||ID||Time)||Time);
16)        同步至医生诊疗区块
17)    Else{继续问诊}}
18)End
```

如算法 1 及图 7 所示，当患者与医生在诊断过程中需要使用本系统进行既往病史的查看和诊断记录查询添加时，与系统交互机制如下：

（1）医生登录医疗系统，系统验证医生的账号密码有效性并反馈登录验证情况。

（2）在需要查看既往病史时，系统跳转至患者权限索要界面，患者需向系统提供其公钥并等待系统进行身份验证，验证成功即可查看患者节点中既往就诊的相关记录，在此期间仅获得查看权限，无任何修改权限。

（3）就诊期间，医生如需向节点上添加新的就诊记录，需进入相应记录创建界面，在此系统对患者私钥进行验证，验证成功后医生获得修改权限，可对本次记录进行调整。

3.2.2 医生与医生在数据共享与学术交流中的系统设计

与患者同理，每位医生对应区块链中的一个区块，记录着医生从医以来的诊断记录，与患者信息相关的部分会在诊治关系结束后对相关敏感个人信息进行相应的加密处理，以保证在分享和浏览时的隐私性。

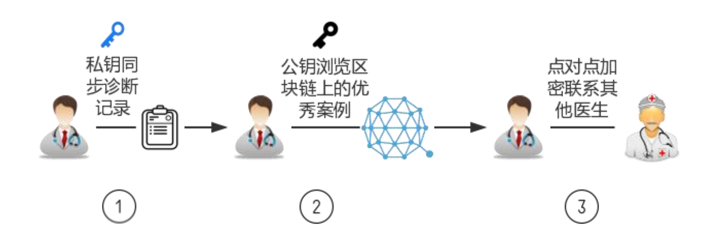


图 8 医生访问系统交互流程图

其过程可用算法 2 表示：

算法 2：医生使用系统交互

1)Begin

2)If（账户状态正常 and 验证 secret_key_doctor）

3) ｛允许登录；获取浏览查看权限；｝

4)While（医生浏览系统）

5) If（深入了解某区块案例）

6) Send request(doctor_ID||Sign(Hash(request)||ID||Time)||Time);

7) 验证 Sign;

8) If（验证通过 and 接受 request）

9) ｛获取对话权限；

10) 对话加密协议生效；｝

11) If（需要远程会诊）

12) Send request(doctor_ID||Sign(Hash(request)||ID||Time)||Time);;

13) 验证 Sign;

14) If（验证通过 and 接受 request）

15) ｛获取视频对话权限；

16) H.235 加密协议生效；｝

17)End

如算法 2 及图 8 所示，当医生在浏览过程中遇到较为感兴趣的病例想要进一步研究或遇到很难解决的医学问题想向其他医院的医生寻求帮助时，可以进行点对点的交流，向该医生发送会诊申请，经过双方同意后，双方（一方）可交换（分享）各自的医疗记录，包括诊治记录，电子影像等文字、图片、影视资料（此处包括医院信息系统、影像归档及传输系统、检验信息系统和放射学信息系统等信息平台记录的患者相关医疗检查的数据）。

如果有必要双方会进行视频连接，通过远程医疗的方式进行远程指导。视频连接过程中，系统支持 H.235 加密协议，确保远程会诊和专家研讨中患者信息的安全。视频结束后的拥有视频资料医生可通过私钥自愿将视频资料上传到区块链平台上。

在点对点的信息交流过程中，两人的对话内容会被进行严格的加密处理，确保交流内容及双方的个人信息不被第三方窃取，以保证医疗信息高效安全地交流。

3.3 系统应用方案设计

结合当今患者在就医时遇到的涉及就医资料方面的困难和阻力，以及远程医疗系统的发展和基于区块链技术的医疗系统在中国应用的前景，将二者结合使查看既往病史、跨地域医疗诊治与医学学术交流等的医疗活动更加安全、便利、系统地进行。

在日常生活中，患者到使用本系统的医院进行就医时，其流程大体如下（图 9）：

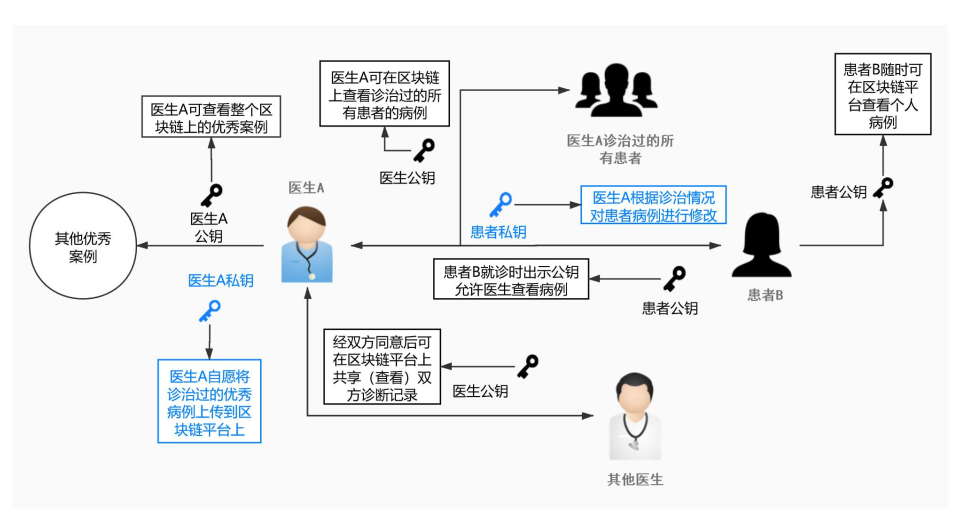


图 9 患者就医时系统使用情景模拟

（1）患者 A 到使用本系统的医院就医时，向医生 B 出示公钥。

（2）医生 B 通过公钥查看 A 的既往病史，了解其身体状况和体质等相关信息。

（3）简单问诊后，患者 A 向医生 B 提供私钥，使得医生能够将就诊记录添加至患者所在区块。

（4）就诊结束后，系统自动更新患者公钥，以保证隐私安全。

如果在此过程中，医生遇到较为棘手的疾病而缺少就诊经验时，可浏览区块链中其他加密处理后共享的案例，根据需求与相应的医生进行交流，从而弥补自身知识的局限性，提高医生诊治的治愈率。

其过程描述如下：

（1）医生在诊治病人时，利用自己的私钥同步诊断记录，自愿选择是否分享自身诊治成功案例。

（2）医生利用公钥登录，浏览区块链上的加密共享案例。

（3）若需进一步了解病例的诊治情况，通过点对点加密的联系方式，与相应的医生取得联系。

至此，在保留原有的医院医疗数据系统和远程医疗系统的基础上，较合理地利用区块链技术对二者进行完善，同时在数据共享方面，不仅实现了原有医疗系统无法实现的功能和远程信息交互，相较于现有的数据共享平台，其安全性得到了进一步保障，为整个医疗系统的信息交流提供了安全可靠的平台。

4 结束语

本文将区块链技术与医疗信息系统相结合，提出基于区块链技术的医疗电子病历大数据共享方案。方案可以保护医生与患者双方的个人隐私，形成双方各自独立的诊断记录，并且具有开放共享、安全交互的特点，可以在一定程度上缓解我国东西部医疗资源差异过大，患者看病难、转院难、就医难的问题，有助于深入进行医疗领域改革、建设更和谐高效的医疗环境。

参考文献

[1]Ekblaw A , Azaria A , Halamka J ,et al.A Case Study for Blockchain in Healthcare : ″ MedRec ″ prototype for electronic health records and medical research data[J]. 2016.

[2]Xiao Y, Huiju W, Dawei J, et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control[EB/OL].https://doi.org/10.1007/s10916-016-0574-6.August 2016.

[3]Shrier A, Chang A, Diakun-thibault N, et al. Block chain and HealthIT:Algorithms,Privacy,and Data.[EB/OL].https://doi.org/10.13140/RG.2.2.36163.91683.August 2016.

[4]徐健,陈志德,龚平等.基于区块链网络的医疗记录安全储存访问方案[J].

计算机应用,2019,39(05):1500-1506.
[5]BAXENDALE G. Can blockchain revolutionise EPRs[J].ITNOW,2016,58(1):38-39.
[6]沈晓利,樊红彬.浅谈医院信息系统中电子病历的实现与应用[J].世界最新医学信息文摘 ,2017,17(89):239+250.
[7]汪鹏,吴昊,罗阳等.医疗大数据应用需求分析与平台建设构想[J].中国医院管理，2015,35（06）:40-42.
[8]孟琳,马金刚，刘静等.医疗大数据的应用与挑战[J].医疗卫生装备，2018，39（10）:71-74+88.
[9]董黛莹，汪学明.基于区块链的电子医疗记录共享研究[J].计算机技术与发展，2019，29（05）：121-125.
[10]吕琦.区块链技术在医疗领域中的应用研究——以健康档案数据保护为例[J].网络空间安全,2018,9(08):18-24.
[11]费禹,宁静,胡青.基于区块链的日志存储系统[J].网络空间安全,2018,9(06):80-85.
[12]薛腾飞,傅群超,王枞,王新宴.基于区块链的医疗数据共享模型研究[J].自动化学报,2017,43(09):1555-1562.

作者贡献说明：

刘曙霞：研究设计，调研数据收集，论文撰写

杨斯博：研究设计

王琰：论文撰写

杨爽：论文撰写

王雅晴：论文撰写

胥美美：论文审阅与修改

安新颖：论文审阅与修改